扫一扫，关注官方微信

## 联系我们


地址：北京市海淀区西二旗大街 39 号 A 座四层

电话：86-10-57933600

传真：86-10-57933600

咨询热线：400-898-1617

网址：www.esafenet.com



亿赛通

ESAFENET

# ESAFENET

亿赛通企业月刊　　中国数据安全防护专家　　www.esafenet.com

5 月刊

2019 年共 11 期



关注企业官方微信

# Esafenet
# Monthly magazines

中国数据安全防护专家

主办：亿赛通

策划：市场部

北京亿赛通科技发展有限责任公司

地址：北京市海淀区西二旗大街 39 号 A 座四层

电话：86-10-57933600

传真：86-10-57933600

咨询热线：400-898-1617

网址：www.esafenet.com




## CONTENTS目录

# 等保 2.0 正式发布，亿赛通五月刊细说信息安全发展新形势

随着我国“互联网 +”战略的逐步落地，云计算、大数据、人工智能、物联网等新技术在关键信息基础设施中广泛应用，网络安全形势与需求发生快速变化，使得等保 1.0 已不再符合要求。五月中旬，等保 2.0 国家标准正式落地，《网络安全等级保护》是党中央、国务院决定在网络安全领域实施的基本国策。作为我国非涉密领域的网络安全基本防护框架，在应对新形势、满足新要求、针对新风险、扩大新内容方面，从政策、标准体系层面都迈入 2.0 时代。此标准的发布对于加强信息安全保障工作、维护网络空间主权和国家安全、提升信息安全保护能力具有重要意义。整个信息安全行业需求将在 2019 年迎来重要改善……



刊首语 PREFACE

国内

## 1、网信办制定个人信息收集规则：杜绝数据泄露需要严打严管


摘要：近日网信办发布了《关于征求意见的通知》。针对当下很多手机应用过渡收集用户信息的乱象，规定了 7 种情况视为违规收集个人信息。

## 2、重庆网警：某医院未履行等级保护制度被罚款 1 万元


摘要：近日，重庆永川某私立医院服务器突然陷入瘫痪，医院业务全面“停摆”，重庆永川公安接警后立即按照“净网 2019”工作要求，启动网络安全应急响应预案，经过民警和技术专家调查核实，该私立医院因未按照网络安全等级保护制度的要求履行安全保护义务。





## 3、上市工业公司披露：子公司服务器突遭黑客攻击


摘要：据深交所网站 5 月 8 日晚间披露，东方精工公告称，旗下子公司北京普莱德新能源电池科技有限公司北京和溧阳的服务器突遭黑客攻击，目前情况未知。东方精工已第一时间发函要求普莱德管理层详细了解黑客攻击的情况（包括文件丢失或损毁的范围和程度），并向东方精工报告。

## 4、网易邮箱回应大量账号被叫卖：仅涉及邮箱地址 已报案


网易免费邮箱 V
5月7日 13:39 来自 iPhone客户端
声明

针对有媒体报道称“在某交流平台，有人公开叫卖网易邮箱账号”一事，网易邮箱说明如下：

1. 经查，报道中提及的违法行为，仅涉及邮箱地址，不涉及用户敏感信息，请大家不要担心。

2. 我们已第一时间向公安机关报案，并正在积极与警方联动，共同打击此违法犯罪行为。

3. 网易邮箱始终珍视用户信息安全，对于危害用户权益的行为，一贯持高警惕、零容忍、强打击的态度，尽全力保护用户权益。每年，网易邮箱投入上亿元经费研发各类安全防御系统，每年成功拦截各类攻击超过50亿次，是国内反垃圾水平最高、效果最好的电子邮箱产品。今后我们会持续加大在信息安全保护的投入力度，请大家放心使用。

4. 用户使用邮箱过程中遇到各类问题，均可通过客服邮箱ketu@188.com或登录在线客户通道help.mail.163.com进行反馈或投诉。同时，我们即将开通24小时服务热线，及时处理用户关切的问题。

摘要：针对媒体报道的“大量网易邮箱账号遭公开叫卖”，网易邮箱在其官方微博上发表声明称，经查，报道中提及的违法行为，仅涉及邮箱地址，不涉及用户敏感信息，并已第一时间向公安机关报案。

## 5、工信部：一季度共处置网络安全威胁 967 万余个

摘要：从工信部获悉：今年一季度信息通信行业网络安全总体态势依旧严峻，网络安全监管成效持续巩固。具体来看，一季度，公共互联网安全保护形势依旧严峻，恶意程序、各类钓鱼和欺诈网站仍不断出现，全行业共处置网络安全威胁 967 万余个，包括恶意 IP 地址、恶意域名等恶意网络资源近 170 万个，木马、僵尸程序、病毒等恶意程序 698 万余个，网络安全漏洞等安全隐患约 4.8 万个，主机受控、数据泄露、网页篡改等安全事件约 93.5 万个。

## 6、易到用车服务器遭攻击，核心数据被加密，攻击者索要巨额比特币


摘要：2019 年 5 月 26 日凌晨，易到用车服务器遭到连续攻击，因此给用户使用带来严重的影响。攻击者索要巨额的比特币相要挟，攻击导致易到核心数据被加密，服务器宕机。目前相关技术人员正在努力抢修。





国外

## 1、FBI 指控网络犯罪头目试图从全球 44000 台电脑中窃取 1 亿美元


摘要：美国联邦调查局（FBI）和全球执法合作伙伴上周四上午称，一名策划了一项犯罪阴谋的网络黑客头目已被逮捕，该阴谋闯入了 44000 台电脑，可能窃取了数百万美元。

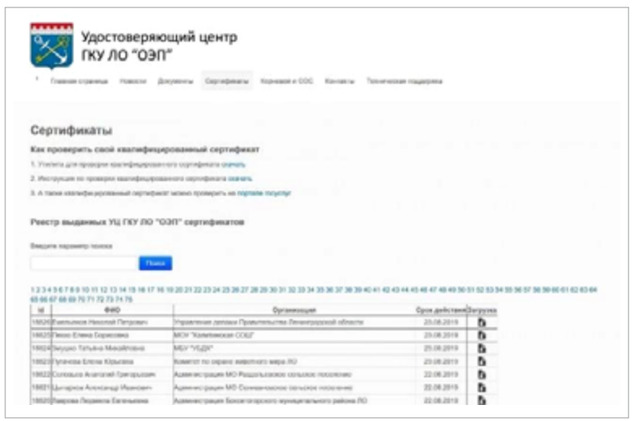
## 2、Stack Overflow 证实遭黑客入侵：客户数据未遭泄露

摘要：开发者知识共享网站 Stack Overflow 证实黑客入侵了其电脑系统，但表示客户数据并未受到影响。Stack Overflow 工程副总裁玛丽·弗格森（Mary Ferguson）写道，“上周末，Stack Overflow 电脑系统受到攻击。我们已经确认，5 月 11 日获得了一定程度的制作访问权限（production access）。”“我们发现并调查了被访问的范围，目前正在解决所有已知漏洞，” 弗格森说，“我们还没有发现任何客户或用户数据被泄露的情况。”对这起黑客入侵事件的调查正在进行之中。

## 3、优衣库母公司顾客信息遭泄露的背后，还有多少数据在裸奔？


摘要：继 Facebook 深陷“数据泄露门”，优衣库母公司日本迅销超过 46 万名顾客信息遭泄露，又令公众对个人信息泄露多了几分担忧。虽然优衣库方面很快向媒体说明，此次事件不涉及中国的网站及信息平台，但仍给国内信息安全敲响警钟。

## 4、俄罗斯政府网站泄露 225 万用户护照和个人信息




摘要：多个俄罗斯政府网站泄露了超过 225 万公民、政府雇员和政治家的个人和护照信息，任何人都可以下载。





## 5、“三只小猫”漏洞威胁全球数百万思科路由器


摘要：美国 Red Ballon 安全研究公司近日发布了一份报告，公布了思科产品的两个漏洞。第一个漏洞被称为 Thrangrycat，允许攻击者通过现场可编程门阵列（FPGA）比特流操作完全绕过思科的信任锚模块（TAm）。第二个是针对 Cisco IOS XE 版本 16 的远程命令注入漏洞，该漏洞允许以 root 身份执行远程代码，通过链接三只小猫和远程命令注入漏洞，攻击者可以远程持续绕过思科的安全启动机制，并锁定 TAm 的所有未来软件更新。

## 6、Choicelunch 高管因窃取竞品客户信息被捕，数百名学生数据泄露

摘要：在 FBI 经过一年的调查后，一位加利福尼亚州的企业高管因为入侵竞争对手网站、窃取客户信息而被捕。然而这位高管并不是来自高端的科技或金融企业，这就是一家为美国学校提供午餐的公司。Choicelunch 首席财务官 Keith Wesley Cosbey 今年 40 岁，上个月被其竞争对手 The Lunch Master 起诉非法获取自己的客户细节信息，这些信息涉及旧金山湾区的年轻人喜欢吃什么，以及对什么食物过敏。Cosbey 被控诉的罪名包括非法登录、欺诈以及身份盗窃。如这些归罪名成立，他将面临着三年的牢狱之灾。

## 7、美国巴尔的摩市政网络遭勒索软件攻击


摘要：美国巴尔的摩市政网络 5 月 7 日遭勒索软件攻击后下线。攻击没有影响警察、消防和紧急反应系统，但市政府的其它部门都在某种程度上受到冲击。市政府的首席信息官 Frank Johnson 在新闻发布会上证实，攻击他们的勒索软件是 RobbinHood。

## 8、Freedom Mobile 数据泄露影响了数千名客户


摘要：加拿大主要电信提供商 Freedom Mobile 公布了一项数据泄露事件，可能泄露了属于数千名客户的敏感信息。周二，来自 vpnMentor 的网络安全研究人员 Noam Rotem 和 Ran Locar 表示他们能够访问属于加拿大第四大电信公司的数据库，该数据库“完全没有受到保护且未加密”。





## 9、因数据泄露而被罚款 449000 欧元


摘要：自去年 5 月数据保护基本法规 (DSGVO) 生效以来，各国的数据保护专员已根据媒体报道至少处以 75 项罚款。根据对“Welt am Sonntag”的调查，总金额为 449,000 欧元。

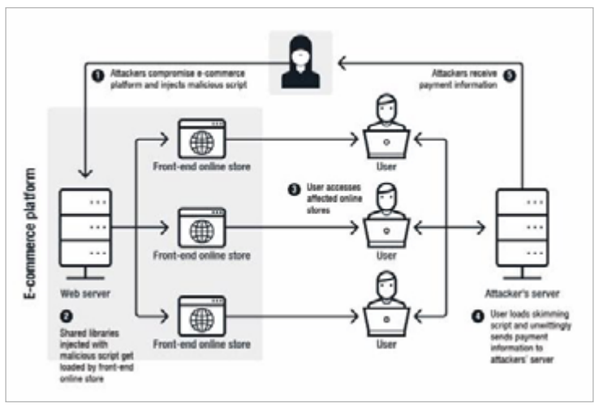
## 10、涉及 2.75 亿条印度公民信息的 MongoDB 数据库被曝光和公开索引


摘要：援引外媒 Security Discovery 报道，他们于 5 月 1 日发现了一个未经保护和公开索引的 MongoDB 数据库，其中包括了涉及印度公民的个人身份信息的 275,265,298 条记录。这些信息中包括姓名、电子邮件地址、性别、教育水平和专业领域、专业技能和职称、手机号码、就业经历和当前雇主、出生日期以及当前的薪资水平。

## 11、美国数据泄露严重！美国两地占比超过全国所有数据泄露的 90%

摘要： 在 2019 年第一季度发布的一份关于数据泄露的报告中显示，美国 1 月份超过 5 亿条数据被曝光，这些数据泄露事件使数十亿份文件遭到盗窃，而纽约和加利福尼亚是数据泄露最严重的两个地区，占比超过全国所有数据泄露的 90%。

## 12、黑客窃取美国和加拿大 201 家校园在线商店的数据




摘要：一群黑客已经种植了恶意 JavaScript 代码，窃取了加拿大和美国大学和学院使用的电子商务系统中的支付卡详细信息。网络安全趋势科技在周五发布的一份报告中称，这些恶意代码发现于 201 家网上商店，这些商店为美国 176 所大学和 21 所加拿大大学提供服务。

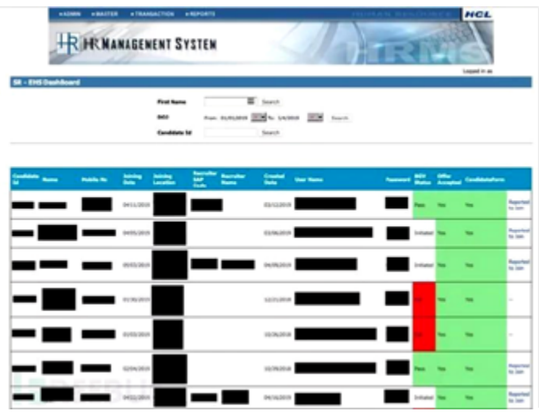




## 13、神秘数据库泄露 8000 万美国人的个人数据


摘要：据外媒报道，一个神秘数据库暴露了近 8000 万美国人的个人信息，影响了 65% 的美国家庭。安全研究人员 Noam Rotem 和 RanLocar 发现了在微软云服务器上托管的 24 GB 数据库。该数据库包含美国家庭的高度敏感信息，其中包括家庭成员的全名、婚姻状况、收入、年龄等。

## 14、福布斯全球 2000 强企业 HCL 泄露大量员工和商业信息




摘要：近日，UpGuard 研究团队发现位列福布斯全球 2000 强的 IT 服务和咨询公司 Hindustan 计算机有限公司（HCL）存在信息泄露的风险。HCL 在多个子域上托管了可公开访问的页面和 Web 界面，导致大量员工和商业信息公开暴露。

## 15、三大安全公司遭黑客攻击？趋势科技承认 赛门铁克否认

摘要：Fxmsp 是一个破坏私人企业和政府信息的俄罗斯组织，近日，该组织生成获取了三家安全公司所有的企业名单，包括：趋势科技、赛门铁克（Symantec）和迈克菲（McAfee）。

## 16、车牌识别器制造商遭受黑客攻击，被盗文件达数百 GB


摘要：据外媒报道，Perceptics 公司是一家提供车牌识别器、车牌识别系统和车辆识别产品的公司。该公司遭到黑客入侵，内部文件被窃取，文件名和附带目录总数量近 65000 ，包括商业计划、财务数据和个人信息。被盗文件达数百 GB，包括 Microsoft Exchange 和 Access 数据库、ERP 数据库、HR 记录、Microsoft SQL Server 数据存储等。





## 17、Canva 1.39 亿用户数据泄露

摘要： 自称 GnosticPlayers 的黑客声称窃取了澳大利亚网站 Canva 的 1.39 亿用户数据。Canva 是一个非常受欢迎的平面设计服务，Alexa 排名在 200 以内。黑客窃取的数据包括了用户名字、真名、电邮地址、城市国家信息，其中 6100 万用户有哈希密码，其他用户的信息还有用于登陆的 Google 令牌。有 7800 万用户使用了 Gmail 地址。

## 18、黑客使用 NSA 黑客工具攻击美国政府网络


摘要：据外媒报道，美国马里兰州巴尔的摩市遭受严重的恶意软件攻击，攻击持续了近三周，导致政府电脑、电子邮件无法使用，房地产销售、水费账单等服务中断。黑客曾利用 NSA 的黑客工具，进行了一些破坏性极强的攻击，如 WannaCry、NotPetya 等。该工具利用未安装补丁的系统，允许攻击者获得系统访问权，并使用恶意软件接管网络中的其他系统。

# 亿赛通受邀出席绿建沙龙，为建筑行业数据安全建言献策


为贯彻落实住建部《建筑节能和绿色建筑发展“十三五”规划》、《辽宁省绿色建筑条例》要求，积极助推大连市绿色建筑相关产业发展，提升绿色建筑水平，大连市绿色建筑行业协会特于 5 月 22 日召开绿建沙龙 -- 绿色建筑活动。协会自成立以来，秉承着“以科技为本，发展绿色健康建筑“的宗旨，聚集了国内多家知名建筑行业单位。

此次会议邀请绿色建筑行业专家、建筑单位、设计院领导代表等几十人共同出席活动。亿赛通作为国内一流的数据安全服务商，荣幸受邀于会中介绍专业的数据安全解决方案，并积极结合现实具体情况为大连市推进建筑行业数据安全更高水平发展建言献策。





“十三五”规划提出建设美丽中国，为“绿水青山”打响了“蓝天保卫战”，不过，绿建过程中企业的数据安全问题同样不容忽视。特别是目前信息化发展迅速，互联网、物联网、云计算等新技术普遍应用，导致企业运营产生大量电子数据，这些数据是新世纪的石油和矿产，若丢失、被盗等均会影响企业的稳定发展，造成经济损失。为此，亿赛通安全专家现场分别从安全行业现状、企业整体方案等方面，全方位分享了亿赛通的数据泄露防护产品与专业方案。


如何防护大数据时代下的数据安全？在新的安全形势下，亿赛通以数据为中心，通过在安全技术领域独特的创新优势，自主研发了终端数据防护、网络数据防护、存储数据防护、应用数据防护、介质数据防护等安全产品，并针对特定细分行业领域，实现“智能识别、智能加密、智能审计、智能阻断”的一体化安全管理。在建筑行业中已先后为华润置地、万科、中国建筑设计院、中国城市规划设计院等国内众多知名企业提供数据安全解决方案。

随着国家相关法律法规出台，欧盟 GDPR（通用数据保护条例）的颁布，加强数据防护不仅是企业发展的根本需求，更是企业的一份责任和义务。大数据时代，保护数据安全异常重要，亿赛通坚持用大数据构建“大安全”生态，利用前沿技术对企业敏感数据进行识别，提高敏感数据的识别精度，从而进行全方位智能防护。

## 典型客户案例

1、中国城市规划设计研究院
2、华润置地有限公司
3、中国建筑设计研究院
4、中国建筑标准设计研究院
5、内蒙古电力勘测设计院
6、广东省城市规划设计研究院
7、重庆电力设计院
8、江苏省邮电规划设计院
9、河南交通规划设计研究院
10、中国能源建设集团安徽电力设计院
11、中国能源建设集团甘肃电力设计院
……

# 持续发力 --2019 年亿赛通华中区渠道大会取得丰硕成果


## 2019 年华中区渠道大会圆满落幕

以“携手同心，共赢未来”为主题的 2019 年亿赛通华中区渠道大会已于 5 月 29 日 -5 月 30 日顺利召开。在经历了华南区、华东区等地渠道会成功举办后，亿赛通的品牌效应不断发酵，其核心产品及渠道政策也受到了众多渠道伙伴的关注。

因此我们乘胜追击，渠道大会第三站（华中区）吸引了当地众多合作伙伴到场支持。会中共同探讨大数据时代的安全问题，解决数据管理痛点，为国内数据安全保驾护航。





二十一世纪，云计算、大数据等新技术发展迅猛，数据信息已成为企业的黄金资产，如何提升企业的数据管理能力，是 IT 建设工作的重中之重。

此次华中渠道大会旨在搭建一个线下合作对接平台，与渠道伙伴对接信息、搭建人脉。活动中进行了全国渠道招募政策解读，最新产品技术详解，并在会议结束前对到场技术人员进行了严格的培训考试。




## 产品解读篇

亿赛通技术专家与现场嘉宾共同交流数据安全常识和数据泄露防护的重要性。大数据的发展是一把“双刃剑”，其运用已经渗入到我们生活的方方面面。一方面大数据使人们的生活变得更加便利，给人们提供的个性化服务会更加贴心。另一方面信息一旦被泄露、被恶意利用，也会造成极大的危害。如何有效地保护客户的数据，成了企业面临的巨大的挑战。亿赛通专注自主研发的数据泄露防护产品，经过不断更新、完善、优化后，可满足企业客户多维度的安全需求。

## 行业分析篇

亿赛通专业人士现场还分享到，客户对于数据安全的需求不断提高，行业需求将进一步趋于成熟，如制造、研发、金融等专有市场信息安全需求更加强烈。另外，政府重视和政策扶持也不断推动信息安全产业的快速发展。尤其各大法律条文的出台，更是将数据保护提到了法律高度，加强数据安全是行业大势，势不可挡。

五月中旬，等保 2.0 正式发布，意味着我国数据安全行业将进入新形势。亿赛通现场就新形势下的数据安全解决方案达成交流，并通过品牌宣讲及客户案例的展示，联合向渠道伙伴们展示了公司在数据安全领域的实力与保障。

## 技术认证篇

为了更好地进行技术及业务交流、加强与渠道伙伴的开放合作，此次华中渠道会特设技术认证考试环节，亿赛通的技术专家在现场与嘉宾进行面对面答疑解惑，与渠道合作商就公司的产品与区域业务推广策略进行了深入交流，并围绕亿赛通的最新产品优化与研发，探寻数据安全发展的时代变革，共同助力国家数据安全的创新与发展。



数据安全威胁是动态和变化的，仅仅依靠传统的防御观念，已经不适应当前的数据安全环境，必须树立动态、综合的防护理念。通过针对性的解决方案和运营服务，才能实现最终安全的落地。并且关键数据的丢失就意味着企业走向衰亡，而数据如何安全存储更是对未来企业提出的必备要求，因此安全市场必将有愈发光明的前景。在这个过程中，亿赛通一直在努力，不断研发出更符合客户需求的解决方案，确保核心数据安全，保护数据安全道路上，我们与您同行。





# 划重点！等保 2.0 正式实施……


图一：等保 2.0 架构变化

近年来，伴随着信息革命的飞速发展，网络空间正逐步成为信息传播的新渠道、生产生活的新空间、经济发展的新引擎、社会治理的新平台。《信息安全等级保护管理办法》作为我国网络安全建设的重要指导依据，从首次被提出至今，逐步筑起了国家网络和信息安全的重要防线。然而随着云计算、物联网、移动互联、工业控制、大数据等新领域的发展，原有的标准已不能满足等级保护的工作需要。

现《网络安全等级保护制度 2.0》已正式发布，等保 2.0 涵盖云计算、大数据、物联网、工控网络等新场景下的安全要求，在安全防护思路上相比于传统安全体系有极大的突破，必将成为迎接新时期网络安全建设的新基础。

从 2014 年 3 月开始，由公安部牵头组织开展了信息技术新领域等级保护重点标准申报国家标准的工作，并从 2015 年开始陆续对外发布草稿、征集意见稿。之后网络上开始有了“等保 2.0”的叫法，“等保 2.0 的主要区别是新技术要求”，这种理解借助互联网在网络迅速蔓延，一夜之间成为当前社会主流认知。

## 等保的架构变化

从等保 1.0 到 2.0，安全通用要求目录分类由物理安全、网络安全、主机安全、应用安全、数据安全及备份恢复、安全管理制度、安全管理机构、人员安全管理、系统建设管理、系统运维管理，变更为为安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理。其中，等保 1.0 中网络安全在等保 2.0 划分为安全通信网络及安全区域边界两部分; 等保 1.0 中主机安全、应用安全、数据安全及备份恢复在等保 2.0 中调整为安全计算环境。

## 等保 2.0 提出的新标准

“等保 2.0”新标准将会对网络安全带来重要改变，等级保护工作也将面临显著的变化，本次从两个方面进行解读。

### （一）定级对象范围

“等保 2.0”新标准中，每一级除通用要求外，均还新增了云计算安全、移动互联安全、物联网安全、工业控制系统安全和大数据安全这 5 个扩展要求，以应对新兴技术安全需求。

相比“等保 1.0”将定级对象统一定义为信息系统，《网络安全等级保护定级指南》对定级对象的具体范围根据扩展要求进行了细化：

**云计算平台方面：**定级对象将区分为服务的提供方和租户方；

**物联网方面：**感知、网络传输和处理应用等特征因素不单独定级，将作为一个整体进行评定；

**移动互联方面：**移动终端、移动应用、无线网络、相关有线网络业务系统等也将统一定级；

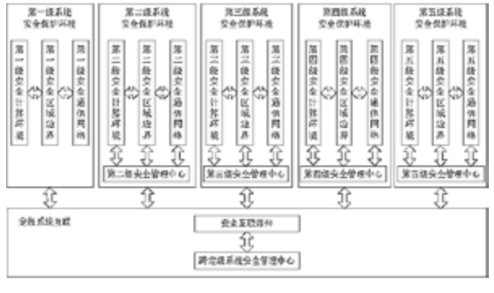
**大数据方面：**安全责任主体相同的平台和应用将整体定级，除此之外为单独定级。

网络运营者在实施定级工作时，首先应当确定自身作为定级对象满足的基本特征，若从事基础信息网络、工控系统、云计算、物联网、大数据等特定领域服务的，还应符合相应的要求。

### （二）新概念的强化

在等保 2.0 中，引入了“可信”、“安全运维”和“安全管理中心”三个新概念。可信计算是在计算和通信系统中广泛使用基于硬件安全模块支持下的可信计算平台，以提高系统整体的安全性。《网络安全等级保护基本要求》（报批稿）中强化了可信计算，充分体现一个中心、三重防御的思想，由被动防御变成主动防御，并强化可信计算安全技术要求的使用。


图二：等级保护安全框架



图三：网络安全等级保护安全技术设计框架





## 等保 2.0 与网络安全法的关系

等保 2.0 的标准是国内非涉密信息系统的安全集成标准，网络安全法是作为法律、中国信息安全的基本法。网络安全法中明确的提到信息安全的建设要遵照等级保护标准来做建设。

网络安全法从立法到配套法律法规的确定完善，到市场上反映出来一定的效果是需要一定的过程的。这个过程在于执法是否落实到位，规定的标准是否真的符合业务安全痛点。目前来看市场上大部分单位都以合规性建设为主，从立法角度来看，是一部非常健全的体系，会使业务的风险管控、网络安全能力会上升到一个新的高度。

等保 2.0 既是国家安全部署要求，也是市场发展客户安全保障的刚需，还是企业品牌树立、可持续发展的重要保障。等保 2.0 的落地实施是一个涉及到多环节、体系化的工作，作为国内专业的数据安全厂商，亿赛通一直密切关注等保 2.0 的进程，关注相关法规标准、市场动态，后续针对各个场景进行深入解读，敬请期待。

# 网易邮箱遭“打脸”，百万邮箱账号仅值 50 元?

对于绝大多数人来说，邮箱不仅是日常收发邮件，更多的时候，是作为一个安全验证工具在使用。也就是说，即便你的邮箱中没啥机密，但是一旦被黑客盗取，你用这个邮箱注册的所有账户都有被盗的风险。

## 网易邮箱百万账号泄露

近日，在某交流平台，有人公开叫卖网易邮箱账号，百万邮箱售价仅 50 元。卖家自称可向这些邮箱发送营销信息，并展示了据说包含有百万个邮箱账号的文件。测试后反馈信息显示，仅有 6 个邮箱发送失败。网易邮箱内部人士证实，如果没有退回，证明网易邮箱账号中心存在这个账号，也就是说账号真实存在。

如今，信息交易黑市已经出现数据定制服务和一条龙服务，信息外泄原因主要是平台服务器安全措施等级低，很容易被黑客入侵；黑客通过软件漏洞进行攻击；公司内部人贩卖用户信息。

卖家也挖掘到网易邮箱的商机，她将邮箱卖给不同商户，每天都有资金入账，盈利模式稳定。“我赚的最多的时候，一天挣了买一台 iphone7 的钱。”随后，卖家提供的截图显示，一名卖家花 1000 元，向她购买 500 万条数据，已支付 500 元订金，约定当晚交货。“只要你能付得起钱，我能提供足够数据，能卖的数量能让你‘倾家荡产’。”

## 违法获取数据可定罪

在卖家看来，通过爬虫技术获取网易邮箱并进行交易不违法，“爬虫程序是我男朋友做的，爬取的是网络上公开信息，不涉及违法行为。”

“爬取数据的合法性其实很窄，只有不妨碍网站的正常运行、严格遵守网站设置的 robots 协议，不强行突破网站的反爬措施，这才是真正合法的数据爬取行为。”安全专家表示，从法律角度来看，虽然数据的爬取是从公开数据当中进行数据抽查，但如果使用不当，也会突破法律的边缘。

《网络安全法》第四十二条规定，网络运营者不得泄露、篡改、毁损其收集的个人信息；未经被收集者同意，不得向他人提供个人信息。但是，经过处理无法识别特定个人且不能复原的除外。网络运营者应当采取技术措施和其他必要措施，确保其收集的个人信息安全，防止信息泄露、毁损、丢失。在发生或者可能发生个人信息泄露、毁损、丢失的时候，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。






网易免费邮箱
5月7日 13:39 来自 iPhone客户端
声明

针对有媒体报道称“在某交流平台，有人公开叫卖网易邮箱账号”一事，网易邮箱说明如下：

1. 经查，报道中提及的违法行为，仅涉及邮箱地址，不涉及用户敏感信息，请大家不要担心。

2. 我们已第一时间向公安机关报案，并正在积极与警方联动，共同打击此违法犯罪行为。

3. 网易邮箱始终珍视用户信息安全，对于危害用户权益的行为，一贯持零容忍、零容忍、强打击的态度，尽全力保护用户权益。每年，网易邮箱投入上亿元经费研发各类安全防御系统，每年成功抵挡各类攻击超过50亿次，是国内反垃圾水平最高、效果最好的电子邮箱产品。今后我们会持续加大在信息安全保护的投入力度，请大家放心使用。

4. 用户使用邮箱过程中遇到任何问题，均可通过客服邮箱kefu@188.com或登录在线客户通道help.mail.163.com进行反馈或投诉。同时，我们即将开通24小时服务热线，及时处理用户关切的问题。

另外，《电信和互联网用户个人信息保护规定》第十条规定，电信业务经营者、互联网信息服务提供者及其工作人员对在提供服务过程中收集、使用的用户个人信息应当严格保密，不得泄露、篡改或者毁损，不得出售或者非法向他人提供。

《“两高”关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》规定了较低的入刑门槛——该司法解释将个人信息根据敏感度的高低分为三档，非法出售的数量分别达到 50 条、500 条、5000 条，或违法所得达 5000 元以上即可定罪，如果是在履行职责、提供服务过程中“监守自盗”的，标准减半。

企业若要实现数据合法获取，必须满足两个条件。一是互联网企业只能收集其提供服务所必需的个人信息，非必需信息一概不得收集；二是企业必须明示收集、使用的目的、方式和范围，并征得用户的同意，最常见的形式是平时注册账号前需要打勾的“隐私协议”。

## 如何防止密码被盗

1、千万不要在多个账户使用同一个密码，这会增加密码泄露的风险；

2、将你的邮箱密码升级到强密码，不要使用纯数字，不要使用和账户名一模一样的密码；

3、不要在公共计算机上留下邮箱账户和密码，如果实在要用，一定要记得及时清除账户和密码，防止被有心人利用。

4、启用密码期限管理功能，定期修改密码；

5、在手机应用程序中启动双重身份验证，给你的账户多一重保护；

6、防止其他组织泄露你的个人信息 。

黑客可以同时修改邮箱地址和邮箱密码，之后若想找回密码，则非常困难。现实生活中，很多人使用邮箱地址来注册账户；在网购，注册脸书和推特、Instgrame 等社交账户时，也都会用到邮箱来验证。所以，一旦你的邮箱信息被黑客盗取，其他账户也会面临被盗的风险。尤其是某些马大哈，邮箱账户、密码和其他账户一模一样，这就危险了！中国数据安全防护专家亿赛通温馨提示：一旦邮箱信息泄露，其他账户的密码也就形同虚设。你的个人信息会被泄露，你的资产账户也可能面临风险，甚至可能遭到黑客的勒索！所以，千万不要觉得邮箱账户密码泄露是小事儿 ~

# OMG，信息泄露不分行业，一不小心就“裸奔”


本周，优衣库和英特尔让广大网友舔了好几天的屏。两大行业巨头深陷信息泄露事件，接下来让我们回顾这几天吃过的瓜……

## 讯销集团旗下品牌泄露 46 万客户信息

据网络爆料，优衣库网站遭受黑客攻击，可能导致客户个人信息遭泄露。随后，日本迅销公司发布声明称，旗下品牌优衣库、GU 销售网站逾 46 万名客户个人信息遭未授权访问，造成客户姓名、地址、电话号码和信用卡信息泄露。





迅销称，经调查此次事件仅限于日本网站，不涉及中国的网站及信息平台。这是一次基于列表的攻击，当客户在多个网站上使用相同的用户名和密码组合时，可能会遭受此类攻击。

迅销公司为此次事件向客户致歉，承诺将防止同类事件再次发生。并称一直以来严格遵守国家的各项法律法规，并通过严格的管理流程和技术手段保护消费者的个人信息及消费数据，为消费者提供安全的购物环境。


## 英特尔存在严重安全漏洞

在优衣库事件发酵相隔几个小时后，世界科技巨头英特尔也爆出被黑客袭击的大料：

据外媒报道，英特尔被被曝出芯片安全重大漏洞，代号“ZombieLoad”，译为“ 丧尸 ”。黑客可直接借助该漏洞读取流经英特尔芯片的几乎所有电脑数据；随后更有媒体透露，漏洞的恐怖将波及几乎所有 2011 年装有英特尔芯片的计算机。

也就是说，无论我们用的是苹果电脑还是微软电脑，无论你的计算机多贵，运行都流畅！全都不能幸免，99% 的电脑基本通通将会中招！！！一旦顶尖黑客利用此漏洞，不需要恶意攻击，就能随时入侵你的电脑，并且不留痕迹！！！

一时间，整个科技圈炸锅了……

## 信息交换便利生活

随着科技的发展，手机、电脑让人们的生活越来越便利，各式各样的 APP 与网店应运而生。但你在尽情地享受这便利生活的同时，是否考虑过你的生活在互联网中早已无处遁形？在大数据时代，为了享受信息技术的丰富资源及便捷的产品服务，通常会授权他人使用或查看自己的个人信息，甚至不少人主动在社交软件平台上公开自己和家庭的个人信息。

但从法律层面来看，个人信息仅属于自己所有，信息本质上仍只是授权企业进行审核，企业应依法合理地使用，并做好保密措施，防止他人滥用个人信息。然而现在众多企业却大肆滥用，甚至以出卖的方式泄露。

## 三方合力，力保信息安全

近两年来全国共侦破侵犯个人信息犯罪相关案件 3700 余起，抓获犯罪嫌疑人 11000 余名；全国法院审理利用网络侵犯个人信息犯罪案件已达 1529 件。

国家也抓紧立法，保障个人应有权益：《消费者权益保护法》增加了消费者个人信息依法得到保护的条款；《网络安全法》的实施，将个人信息保护作为一项重要制度；两会政府工作报告提出制定《个人信息保护法》。

面对侵害消费者个人信息愈演愈烈的严峻挑战，必须采取多管齐下，继续完善相关法律法规、加大监管部门惩罚力度，个人需要提高信息保护的意识和能力，行业内部也需要不断加强自律，充分地保护消费者的个人信息权，为社会经济的稳步运行提供良好的信息环境。

信息安全无小事，一个小小的疏忽，就可能会引发不可估量的恐怖后果：随着科技的进步，手机、电脑已经成为了我们生活、工作必不可少的“ 工具 ”，但也导致信息泄露更加容易，中国数据安全防护专家亿赛通提醒您，千万不要认为信息泄露小事，不要等到电脑被黑客入侵了，重要资料被泄露再想起信息安全的重要，到时将后悔莫及！

# 三大安全公司被黑客渗透，30TB 数据失窃损失巨大

听说了吗，安全圈又出大事儿了！

啥大事儿，说来听听

有三家安全公司被黑客组织攻击了，源代码和网络访问权都在安网出售呢！

安全公司还能被攻击？具体情况详细介绍一下呗。



亿赛通小贴士 ESAFENET PROMPT

## Fxmsp 来历

日前，某威胁情报公司发布消息称三家安全公司遭到一个名为 “Fxmsp” 的俄罗斯黑客组织的渗透。据悉，Fxmsp 是一个破坏私人企业和政府信息的俄罗斯组织，该组织自 2017 年开始活跃，过去两年中 Fxmsp 已经通过黑客企业网络赚取了大约 100 万美元。而从 2019 年 4 月开始，该组织就在网络犯罪论坛上声称他们已经渗透了三家反病毒公司，并从这些公司的反病毒软件、人工智能和安全插件中提取了源代码。

## 三大公司 30TB 数据被提取

近日，Fxmsp 黑客组织在俄罗斯暗网论坛中以 30 万美元的价格出售其从三家安全公司处提取的源代码和网络访问权。根据 Fxmsp 提供的截图显示，该组织共计拥有 30TB 的数据。趋势科技（Trend Micro）就是其中之一，该公司也在随后进行了回应：已在第一时间采取行动隔离了受影响的测试实验室网络，并采取额外的保护措施合理地保护了所有相关的环境；赛门铁克（Symantec）是第二家遭遇渗透的企业，但其否认了这一说法；迈克菲（McAfee）是第三家公司，但其表示：没有发现 McAfee 产品、服务或网络受到所述威胁影响的迹象。

## 黑客组织如何运作?

据悉，该威胁组织的运作方式包括利用外部可用的远程桌面协议（RDP）服务器和公开的活动目录账户来访问网络环境，该组织还声称已经开发出了一种能够感染知名企业并窃取其用户名和密码的僵尸网络。

威胁组织引发的这起事件，应引起各大企业的深刻反思，就连防范严密的安全公司都能被黑客入侵，那么你的企业是否需要数据安全防护呢？如果企业存在安全漏洞，并且恰好被攻击者利用，导致服务器被黑客控制。那么企业的办公详情、商业秘密、工作隐私等等数据将赤裸裸的暴露在不法分子眼前，随后他们会从事各种勒索、诈骗、威胁、黑市交易等非法活动，继而对企业造成巨大的损失。

## 亿赛通技术良方专业防止安全隐患

中国数据安全防护专家亿赛通，专注于数据安全防护市场，针对各种数据泄露情况，如操作失误、非法侵入、病毒感染、设备损坏、信息窃取等，在数据的收集、存储、管理与使用等过程进行规范和监管，消除企业安全隐患，从而实现一体化的数据安全防护，有效的防止用户核心信息资产外泄。

## 文档安全管控

以数据透明加密技术为核心，通过信息安全边界的建立，降低核心信息资产的有意或无意泄密风险，如源代码、设计图纸、财务数据、经营分析等。文档透明加密系统遵循加解密透明、管理强制和使用无感知的设计原则，有效防止企业核心信息资产外泄的同时，不影响用户工作习惯及业务效率。

## 文档权限管理

对企业核心电子文档进行细分化的权限设置，确保机密信息在特定授权范围内合法操作，同一文档可以针对不同用户设置不同权限。通过实时权限控制，为用户提供安全授权下的机密信息共享机制，实现机密信息分权限的内部安全共享。

## 文档外发管理

当客户需要将涉密文档外发给客户（代理商、合作伙伴等）时，应用文档外发控制系统生成外发文件发出。在外发文件打开时，用户需通过身份认证，方可阅读文件。同时，外发文件可以限定接收者的阅读次数和使用时间等细粒度权限，从而有效防止客户重要信息被非法扩散。

# 强强联合 | 长电科技携手亿赛通 共推制造业数据安全体系升级

## 关于江苏长电科技股份有限公司

中长电科技成立于 1972 年，2003 年在上交所主板成功上市。历经四十余年发展，长电科技已成为全球知名的集成电路封装测试企业，面向全球提供封装设计、产品开发及认证，以及从芯片中测、封装到成品测试及出货的全套专业生产服务，先后被评定为国家重点高新技术企业、中国电子百强企业、集成电路封装技术创新战略联盟理事长单位、中国出口产品质量示范企业等，拥有国内高密度集成电路国家工程实验室、国家级企业技术中心、博士后科研工作站等。





## 客户需求

作为集成电路封装测试领域全球知名企业，长电科技的文件安全是企业最为重视的部分，不仅是研发部门的核心文件，还包括专利发明、产品著作权等都是公司的重要资产。数据资产把握着企业的经济命脉，为提高企业内部数据的安全性，实现国内与新加坡、韩国和美国等各国之间的文档内容流转安全可控，文档脱离公司管理平台后能有效防止文件的扩散和外泄，长电科技急需建立一套完善的数据安全管理体系。对此，经过与客户反复的技术测试论证，多次讨论、分析后，亿赛通凭借着丰富的项目运作经验和技术优势，成功的击败了全部的竞争对手，与长电科技携手共同保护企业数据资产安全。

## 功能亮点

亿赛通文档安全管理系统防止长电科技内部员工泄密和外部人员非法窃取企业核心重要数据资产。

**智能透明加密：**实现对任意文档自动透明加密的同时，不影响用户的使用习惯；

**内容安全防护：**防止核心数据通过复制拖拽、截屏录制、打印输出以及副本另存等方式泄密；

**安全水印支持：**通过自动添加安全警示及版权标识信息，来降低屏幕录制和自主打印所带来的泄密风险；

**离线办公支持：**可通过离线审核、策略预设及离线补时等功能满足各种离线办公要求；

**开放式策略库：**用户可根据业务及管理需要进行安全策略自定义，开放、灵活的策略配置可降低企业后续维护成本；

**细粒权限控制：**细化外发文档的阅读、编辑、复制、打印等组合权限，并可根据管理需要设定文档生命周期，防止文档的二次扩散。

## 项目成果

亿赛通电子文档安全管理系统目前已成功部署在长电科技江阴本部、滁州、宿迁分部，子集团星科金朋江阴本部以及先进封装，下一步还将部署在韩国、新加坡以及美国子公司，为客户成功实现了公司内部文件可以在所有涉密终端上无障碍流转，促进了客户在项目过程中建立跨部门组织，方便业务交流，安全、高效的完成各项工作，大大的提高了工作效率。同时在数据资产安全保护方面，有效的防止了内部核心信息非法授权阅览、拷贝、篡改等，以达到既防止文档外泄和扩散，又支持内部知识积累和文件共享的目的。

# 招商局重工（江苏）有限公司

## 客户简介

招商局集团是驻港大型企业集团，经营总部位于香港，是中央直接管理的国有重要骨干企业，亦被列为香港四大中资企业之一，连续九年获国务院国资委评为“A”级中央企业，管理总资产 3.59 万亿元。业务包括交通运输及相关基础设施的建设、经营与服务（港口、公路、能源运输、物流等）、金融投资与管理、房地产开发与经营等。



典型案例 TYPICAL CASES

## 需求背景

作为江苏省委省政府及海门市政府重点推进项目，招商局重工（江苏）技术图纸、行政办公、项目文档等资料愈发重要。企业为了防止庞大的业务数据、公司重要信息泄露出去。招商局重工接触了多家数据安全厂商，最终在这些厂商中选择与亿赛通携手合作，共同保障招商局重工（江苏）有限公司的数据安全运行管理。

## 解决方案

电子文档安全管理系统是一款电子文档安全防护软件，该系统利用驱动层透明加密技术，通过对电子文档的加密保护，防止内部员工泄密和外部人员非法窃取企业数据资产，对电子文档进行全生命周期防护。

内容安全管控：截屏录屏控制文档、阅读水印文档、打印水印、 拷贝粘贴控制；

安全分级控制：实现人员密级、数据密级的安全分级管理控制， 满足组织数据分级安全管理要求；

身份认证集成：统一身份认证平台进行无缝集成，如实现组织构架 及用户账号信息的自动完整同步和单点登录认证集成；

安全水印支持：通过自动添加安全警示及版权标识信息来降低屏幕 录制和自动打印所带来的泄密风险。

## 项目成果

亿赛通不仅为招商局重工（江苏）有限公司各业务部门特别是技术中心和研发中心部署合理的电子文档安全管理系统，同时使得该企业相关业务流程更为合理化、流程化、规范化。在数据传输上既保证了内部业务网络较高的可用性、可靠性、保密性，又对内部核心数据有较强的防御和管控能力。